



Use of Employee Owned Information Systems

HIPAA Privacy ♦ October 2005

HIPAA Security IPT, October 11, 2005

ISSUE BACKGROUND

At the August 9, 2005 meeting of the Health Insurance Portability and Accountability Act (HIPAA) Security Integrated Project Team (IPT) the Army service representative, reported that there recently has been a push within Army MEDCOM to use non-government furnished equipment or employee owned information systems (EOIS) and clientless VPNs. His office believes that use of EOIS presents a very high risk to both the Military Health System (MHS) and Army networks and to electronic Protected Health Information (ePHI). He further elaborated that there is no way to validate that an EOIS is IA or HIPAA compliant. In particular compliance with IAVAs and the prevention of spyware, P2P software or malicious logic cannot be validated. EOIS may not employ IA tools such as firewalls, AV software, and strong passwords. Other issues include secure disposal of the hard drive, exposure of ePHI to family members and inclusion of EOIS in the DITSCAP to ensure that the DAA is aware of and approves of its use. Use of EOIS violates a number of Army policies and best business practices (BBP) including AR 25-1, AR 25-2, VPN BBP, Hard Drive BBP, and the Wireless BBP. The Army realizes that there is an operational requirement for remote access but they do not believe that there is an operational requirement to achieve remote access through the use of personal computers. Related to the EOIS issue is the perceived endorsement for using clientless VPN as opposed to client based VPN for remote access. Clientless VPN may be utilized anywhere or anytime including an airport kiosk, coffee shop, internet café or an EOIS. The use of public systems increases the risk for the presence of spyware and sniffers. It is also inappropriate and presents a risk of unauthorized disclosure to access a medical system and conduct work with ePHI in a public place such as an internet café. One of the systems that is being considered for use with CHCS II and is being endorsed by MHS is SPAC, a clientless VPN. The Army believes that this is a violation of both Army policy (AR 25-2) and what is required for compliance with HIPAA because the covered entity has no control over where some one is accessing ePHI.

RESPONSES

The Navy, Air Force, and MHS were each asked to respond to the issue and provide their comments.

Navy

There are no Navy specific policies concerning either of these issues. The Navy does not endorse EOIS and continues to use DISA's policy for remote computing (Secure Remote



Use of Employee Owned Information Systems

HIPAA Privacy ♦ October 2005

Computing STIG). In their response concerning this issue they cite two sections of that STIG included below.

- If the site allows Administrative or End-User access to a system, the remote device must be controlled or owned by a Government entity to allow for confiscation and review at any time. This requirement allows for the review of security vulnerabilities and STIG requirements, as well as determination of possible spillage or harm to the network infrastructure.
- *SM050: CAT II) The IAO will ensure personally owned computers are not used for remote access to a DOD network for administrative or end user access.*

The Navy also does not endorse the use of clientless VPNs because clientless VPNs (including SPAC) use SSL instead of IPSec. They cite DISA's policy that mandates the use of IPSec.

- *(SRC630: CAT II) The IAO will ensure a VPN client supports and is configured for IPSec attributes such as 3DES, Tunnel encapsulation mode, and a FIPS 140-2 approved authentication algorithm.*

The Navy intends to review what is needed to increase their MTF's awareness of this issue.

Air Force

Air Force instructions specifically forbid using private equipment to process Privacy Act data (AFI 33-112, AFI 33-202, and AFI 36-8002).

I. AIR FORCE INSTRUCTION 33-112 25 FEBRUARY 2001 *COMPUTER SYSTEMS MANAGEMENT*

19. Use of Computer Systems

19.2. Do not use privately owned computer systems to:

- 19.2.1. Automate functions in support of the unit's mission.
- 19.2.2. Process classified or *Privacy Act* data.

II. AFI 33-202 Vol 1 *NETWORK AND COMPUTER SECURITY*

4.6. Using Hardware or Software Not Owned by the Air Force.

4.6.1. Contractor-Owned. Contractor-owned or -operated hardware and software must meet all security requirements for government-owned hardware and software....



Use of Employee Owned Information Systems

HIPAA Privacy ♦ October 2005

4.6.4. Privately Owned. Do not use privately owned information systems (i.e., hardware or software) to process classified information. Using privately owned hardware and software for government work is strongly discouraged; however, it may be used for processing unclassified and sensitive information with justification and DAA approval (see AFI 33-112, *Computer Systems Management*; and AFI 33-114, *Software Management*). Justification must include mission requirement, government availability, and rationale as to why privately owned information systems must be used. Approved privately owned information systems contaminated with classified information will be confiscated and sanitized. If unable to sanitize, the DAA will determine the disposition of the information system according to AFSSI 5020. Base approval on the following requirements:

4.6.4.1. The written approval specifies the conditions under which the information system operates. When using a privately owned information system for official work, the system must employ antivirus software, government-owned sensitive information must remain on removable media, and government-owned sensitive information must be marked and protected according to the sensitive category (e.g., Privacy Act, For Official Use Only [FOUO], etc.) program directives. This includes systems maintained at a residence, services accessed, and information transportation method(s) (modem, Telnet, Webmail, and/or physical media used).

4.6.5. Telecommuting. Prior to implementing a telecommuting program, consult AFI 36-8002, *Telecommuting Guidelines For Air Force Reservists and Their Supervisors*. This document is the approval authority for all requirements. Ensure vulnerabilities are assessed, with appropriate countermeasures employed, and documented in the certification and accreditation packages.

5.3. Connection By Stand-Alone System. Connection to an Air Force system/resource, by stand-alone systems or networks within a local enclave or through means other than the DISN (e.g., contractor's facility, etc.) requires approval by the MAJCOM/CC or USAF/CVA. Coordinate requests through appropriate offices and include complete C&A documentation according to DITSCAP and this AFI.

III. AFI 36-8002 1 JULY 1998 *TELECOMMUTING GUIDELINES FOR AIR FORCE RESERVISTS AND THEIR SUPERVISORS*

Privately Owned Equipment.

11.1. Reservists may use privately owned equipment for telecommuting purposes.

11.2. Reservists must agree to install, service, and maintain (at their own risk and expense) any privately owned equipment.

PrivacyMail@tma.osd.mil ♦ www.tricare.osd.mil/tmaprivacy



Use of Employee Owned Information Systems

HIPAA Privacy ♦ October 2005

11.3. The government does not incur any liability or assume costs resulting from the use, misuse, loss, theft, or destruction (to include computer viruses) of privately owned computer equipment resources. (AFI 33-112.)

11.4. Government information must be protected from modification, destruction, or inappropriate release.

11.5. When using privately owned computer equipment, the member will store all government data on appropriately marked removable media.

11.6. PRIVATE EQUIPMENT MAY NOT BE USED TO ACCESS OR VIEW CLASSIFIED MATERIAL OR PRIVACY ACT DATA (AFI 33-112)

The Air Force did not address the issue of clientless VPN's.

MHS IA Program Office

The MHS IA Program has not responded to the request for comments on these issues.

DoD POLICY

The Department of Defense Telework Policy addresses the use of EOIS. In summary it states that regular or recurring telework must be done using government-furnished equipment. "Ad hoc" telework (less than once per pay period) must be approved by supervisors. Personal computer's may be used to work on "limited amounts of sensitive unclassified material" if the files are deleted as soon as they are no longer required. These files are ones that are either created by the user on that EOIS or transferred to the EOIS from removable media since the policy also states that EOIS may not be used to access DoD systems or networks remotely.

- i. Government-furnished computer equipment, software, and communications, with appropriate security measures, are required for any regular and recurring telework arrangement that involves sensitive unclassified data, including Privacy Act data, or For Official Use Only (FOUO) data;
- ii. where employees telework on an **ad hoc** basis, personal computers can be used to work on limited amounts of sensitive unclassified material, on the basis that the teleworker must delete the files as soon as they are no longer required, and verify in writing that he or she has deleted all files containing Department information from personally owned computer hard drives;
- iii. employees who telework may be approved by the Component Designated Approving Authority (DAA) to use their personal computers and equipment for work on non-sensitive, unclassified data consistent with DoD policy. Personal



Use of Employee Owned Information Systems

HIPAA Privacy ♦ October 2005

computers may not access DoD systems or networks remotely. The employee is responsible for the installation, repair and maintenance of all personal equipment;

For the complete policy please see <http://www.telework.gov/policies/dodpolicy.asp>.

DoD 8500.2-I does not specifically prohibit the use of EOIS but it also does not explicitly allow their use either. It does address telework as part of remote access providing associated policy for protection of the session, (e.g. encryption requirements).

EBRU-1 Remote Access for User Functions

All remote access to DoD information systems, to include telework access, is mediated through a managed access control point, such as a remote access server in a DMZ. Remote access always uses encryption to protect the confidentiality of the session. The session-level encryption equals or exceeds the robustness established in ECCT. Authenticators are restricted to those that offer strong protection against spoofing. Information regarding remote access mechanisms (e.g., Internet address, dial-up connection telephone number) is protected.

The DoD Telework Policy and DoD 85002.-I do not specifically address the issue of clientless VPNs.

CONCLUSION

The TMA Privacy Office feels that there is no conflict between the DoD policy and existing Service policy where it exists concerning the use of EOIS. The TMA Privacy Office agrees that EOIS should not be allowed access to MTF networks and applications that use, maintain or transmit ePHI. Those individual's allowed to engage in telework that accesses the MTF network should do so from government issued information systems configured in accordance with DoD and Service policy. TMA Privacy Office recommends that the Services supplement their policy if needed and educate their MTF's to increase their awareness of those policies and restrictions.

There is less specific guidance concerning the clientless VPN issue. While most DoD level policy does not include detailed VPN requirements, the DISA Secure Remote Computing STIG does provide guidance for securing DOD assets within a remote access environment. For end-user access to networks the STIG requires that VPN's utilize approved IPSec attributes and is FIPS 140-2 compliant. This would preclude the use of clientless VPN's that utilize SSL. The TMA Privacy Office recommends that the Services investigate the clientless VPN issue within their respective Service and make their requirements known to the CHCS II program office prior to their selection of a VPN technology for use in that application.

PrivacyMail@tma.osd.mil ♦ www.tricare.osd.mil/tmaprivacy